REMARKS

The Applicants and the undersigned thank Examiner Jung for his time and consideration given during the telephonic interview of October 6, 2005. The Applicants also appreciate the Examiner's careful review of this application.

In connection with a petition and two month extension fee to extend the due date to October 24, 2005 and a Request for Continued Examination filed herewith, consideration of the claim amendments above and the remarks below is respectfully requested. Claims 3-18 have been rejected. Claims 1-2 have been cancelled and Claims 3-18 are pending in this application. The independent claims are Claims 3, 7, and 13. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Summary of Telephonic Interview Conducted on October 6, 2005

The Applicants and the undersigned extend their gratitude to Examiner Jung for the telephonic interview conducted with the Examiner on October 6, 2005. During the telephonic interview, the CEO of the assignee, Mr. James Dalton, and Examiner Jung discussed the state of the prior art that was used to reject the currently pending U.S. patent claims.

Mr. Dalton explained what the independent claims were describing as understood by one of ordinary skill in the art and how they contained elements that were not taught by the prior art of record. Examiner Jung requested Mr. Dalton to explain how the claimed technology was different from a standard prepared by the European Telecommunications Standards Institute. Specifically, Examiner Jung requested Mr. Dalton to explain the differences between European Telecommunications Standards Institute (ETSI) technical standard (TS) 101 321 (hereinafter, the "published '321 standard").

While it was explained to Examiner Jung that he did not use the Published '321 standard to reject any of the patent claims pending in his May 23, 2005 Office Action, Mr. Dalton and the undersigned agreed to provide the analysis that Examiner Jung requested. Mr. Dalton explained to Examiner Jung that this Published '321 standard does not provide any guidance on how to exchange a digital certificate between a server and a client. Additional differences between the standard and the claimed technology are further described below.

After listening to Mr. Dalton's explanation of how the Published '321 standard does not describe each and every element of independent Claim 1, Examiner Jung requested Mr. Dalton to explain how the U.S. Pat. No. 6,526,131 issued in the name of Zimmerman et al (applied by the Examiner in his May 23, 2005 Office Action and hereinafter, the "Zimmerman reference") does not anticipate or obviate the claimed technology.

Mr. Dalton explained that the Zimmerman reference, to one of ordinary skill in the art, teaches a way to have functional capabilities of a dedicated connection using a dial-up connection or another connection method that is only used when needed. The Zimmerman reference describes various ways to use a wake-up call to a remote device to quickly establish a connection, rather than maintaining a dedicated phone line. Further details of the Zimmerman reference will be described below.

Mr. Dalton explained that while the Zimmerman reference does discuss a general teaching that certificate information may be exchanged between a certificate authority (CA) and a client device, the Zimmerman reference, like the Published '321 standard, does not explain how to exchange information between a CA and a client device.

Mr. Dalton explained the both the Zimmerman reference and Published '321 standard both do not provide any teaching of receiving a first message from a client Internet telephony device that comprises an automated request to obtain an identity one of an Internet telephony clearinghouse and Internet telephony routing policy server.

After listening to Mr. Dalton, Examiner Jung indicated that he now understands what the patent claims are trying to protect. Examiner Jung suggested a few changes to the proposed claims to make them more clear to the Examiner (which have been adopted by the Applicants and are in the amended claims presented above). Examiner Jung stated he would take these points discussed by the Applicants under consideration and that he would likely need to conduct an update search of the prior art.

The Applicants and the undersigned request Examiner Jung to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected Claims 3-18 under 35 U.S.C. § 103 (a) as being unpatentable over Zimmerman et al., U.S. Patent No. 6,526,131 (hereinafter the "Zimmerman reference") in view of a printed publication entitled, "Introduction to SSL," (hereinafter the "SSL reference") allegedly published on October 9, 1998 and retrieved from the Internet on May 19, 2004 at: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm.

The Applicants will address each independent claim separately as the Applicants believe that each independent claim is separately patentable over the prior art of record.

Independent Claim 3

It is respectfully submitted that the Zimmerman and SSL references and the Published '321 standard fail to describe, teach, or suggest the combination of (1) receiving a first message via HTTP from a client Internet telephony device that comprises (2) an automated request to obtain an identity of one of an Internet telephony clearinghouse and Internet telephony routing policy server, the request further comprising (3) an automated computer programming variable operation (4) that is set equal to alphanumeric text comprising 'getcacert' and that (5) initiates a search for a certificate authority certificate; (6) responding to the request by (7) transmitting a second message comprising the (8) certificate authority certificate of one of (9a) an Internet telephony clearinghouse and (9b) Internet telephony routing policy server (10) in a Base64 format and (11) encoded in ASCII with content type set to text/html; (12) receiving a third message comprising (13) a certificate request from the client Internet telephony device; (14) responding to the client Internet telephony device request (15) by signing the certificate; and (16) transmitting a fourth message comprising (17) the certificate signed by (18) a certificate authority of one of (19a) the Internet telephony clearinghouse and (19b) the Internet telephony routing policy server, as recited in amended independent Claim 3.

The Zimmerman Reference

The Zimmerman reference describes ways to avoid the need for dedicated PTSN phone lines. Dedicated PTSN phone lines can be phone lines used to keep two computer systems permanently connected for immediate communication between the two systems when required. A dedicated phone line is a simple, convenient and secure way to connect two systems.

Meanwhile, the Zimmerman reference describes a way to have the functional capabilities of a dedicated connection using a dial-up connection or another connection method that is used only when needed. The Zimmerman reference relates to remotely waking up customer premises equipment to cause the latter to initiate communication with a network-based service system.

The Zimmerman reference describes ways to use a wake-up call to a remote device to quickly establish a connection, rather than maintaining a dedicated phone line. The wakeup call is identified by means of a characteristic caller ID or distinctive ring, or, in the event the call is picked up, by rapid call termination, by an in-band signal, or by a predetermined period of silence. All these call characteristics permit the customer premises equipment to recognize wakeup calls on a line also receiving normal telephone calls.

The Examiner refers the Applicants to Column 8, lines 37-45 of the Zimmerman reference that generally describes the use of Secure Sockets Layers (SSLs) to establish secure communications. However, this section of the Zimmerman reference does not provide any further details about how SSL is used. In fact, the Examiner admits that the Zimmerman reference does not teach the specifics of the SSL protocol. See Office Action of August 20, 2004; page 2, paragraph number 4.

In light of this, it is apparent to one of ordinary skill in the art that the Zimmerman reference cannot anticipate nor render obvious a combination of elements noted above, especially (a) receiving a first message via HTTP from a client Internet telephony device that comprises (b) an automated request to obtain an identity of one of an Internet telephony clearinghouse and Internet telephony routing policy server, the request further comprising (c) an automated computer programming variable operation (d) that is set equal to alphanumeric text comprising 'getcacert' and that (e) initiates a search for a certificate authority certificate, as recited in amended independent Claim 3.

The SSL reference

The Examiner admits that the Zimmerman reference does not teach the specifics of the SSL protocol. To make up for this SSL deficiency, the Examiner relies on the SSL reference.

The SSL reference generally teaches the SSL protocol. The SSL provides a summary of steps that are taken during an SSL handshake to establish a secure communications channel. However, the SSL reference does not provide any teaching or description of the contents of

messages that are exchanged between a client device and a server. See the SSL reference on page 6, second full paragraph after the table which states the following:

> "The exact programmatic details of the messages exchanged during the SSL handshake are beyond the scope of this document. However, the steps involved can be summarized as follows (assuming the use of cipher suites listed in Cipher Suites with RSA key exchange):"

Therefore, it is apparent to one of ordinary skill in the art that the SSL reference, like the Zimmerman reference, also cannot anticipate nor render obvious a combination of elements noted above, especially (a) receiving a first message via HTTP from a client Internet telephony device that comprises (b) an automated request to obtain an identity of one of an Internet telephony clearinghouse and Internet telephony routing policy server, the request further comprising (c) an automated computer programming variable operation (d) that is set equal to alphanumeric text comprising 'getcacert' and that (e) initiates a search for a certificate authority certificate, as recited in amended independent Claim 3.

Published '321 Standard

As noted above by the Applicants, the Examiner did not use the Published '321 standard to reject any of the claims in the May 23, 2005 Office Action. However, the Examiner requested the Applicants during the telephonic interview of October 6, 2005 to explain how the Published '321 standard is different from the claimed technology. As a courtesy, the Applicants offer the following explanation in response to the Examiner's request.

The Published '321 standard has the following title: "Open Settlement Protocol (OSP) for Inter-Domain pricing, Authorization and Usage exchange." The Open Settlement Protocol (OSP) defines a standard set of messages that telephone carriers can use to authorize and account for inter-carrier telephone calls over IP networks. OSP messages are usually written in XML (eXtensible Markup Language) using text characters and English words and abbreviations.

Example OSP messages are AuthorizationRequest (a message which defines how to request the IP address corresponding to a telephone number) and UsageIndication (an accounting message which reports how call duration after the call is finished).

The OSP standard does not define any security or cryptographic techniques. However, the OSP standard does mention how OSP messages could be secured with existing cryptographic techniques in three places:

1) The OSP standard in section 5.1, page 13, defines that OSP messages written in XML may be conveyed using the Hyper Text Transport Protocol (HTTP) over an Internet Procotol (IP) network. The OSP standard also states that for secure communications, the OSP messages written in XML may also be transmitted using the Secure Sockets Layer (SSL) or Transport Layer Secure (TLS) protocol.

2) Annex B, page 46, of the OSP standard references cryptographic algorithms required by SSL/TLS and digitally signed messages and tokens.

3) Annex D, page 50, defines the format for OSP authorization tokens which may cryptographically encoded.

While these three security techniques rely on digital certificates, the OSP standard and the reference security technologies (SSL/TLS) do not teach how to exchange a digital certificate between and server and a client. As discussed with the Examiner during the telephonic interview of October 6, 2005, a certificate can be exchanged between a client and a server via any number of obvious mechanisms such as through U.S. Postal service (mail), E-mail, File Transport Protocol (ftp), and other like mechanisms. However, none of these mechanisms are practical for voice over Internet Protocol (VoIP). The inventive claims define an efficient operation which enable a VoIP client to automatically 'enroll' with a certificate authority. Enrollment usually includes obtaining a public key and signed certificate from a certificate authority.

In light of the differences between amended Claim 3, the SSL, Zimmerman references,